(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105354902 B
(45)授权公告日 2017.11.03

(21)申请号 201510757989.5

(22)申请日 2015.11.10

(65)同一申请的已公布的文献号
申请公布号 CN 105354902 A

(43)申请公布日 2016.02.24

(73)专利权人 深圳市商汤科技有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室

(72)发明人 刘祖希 王子彬 张伟 陈朝军 刘亮 肖伟华 马堃 金啸 张广程

(74)专利代理机构 北京中济纬天专利代理有限公司 11429
代理人 张晓霞

(51)Int.Cl.
G07C 9/00(2006.01)
G06K 9/00(2006.01)

审查员 沈芳

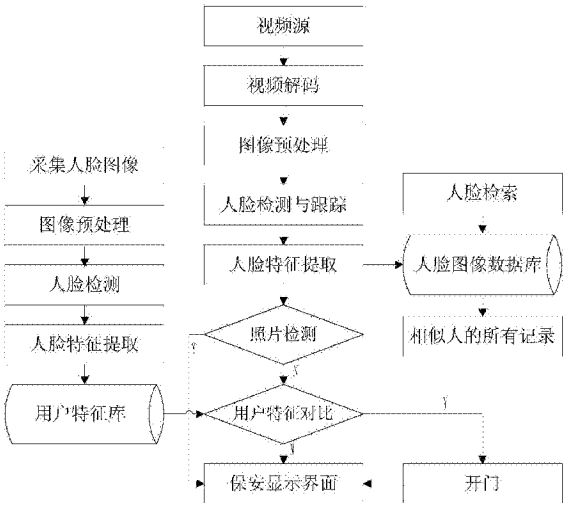
权利要求书3页 说明书8页 附图1页

(54)发明名称

一种基于人脸识别的安保管理方法及系统

(57)摘要

本公开提供了一种基于人脸识别的安保管理方法及系统，所述方法包括建立用户特征库、提取视频帧的图像数据、检测并提取人脸特征、判断是否为照片欺骗、判断是否为合法用户等，通过采用深度学习来识别人脸，可以提供人脸识别的准确度。所述系统基于所述方法实现，包括用户特征库模块、视频帧图像数据提取模块、人脸特征提取模块、照片欺骗判断模块、合法用户判断模块等，通过准确的人脸识别，为安保管理带来方便，有效避免照片欺骗，并对人员进行跟踪。



CN 105354902 B

1.一种基于人脸识别的安保管理方法，其特征在于，所述方法包括下述步骤：

S100、建立用户特征库：收集允许通过门禁的合法用户的用户信息，所述用户信息包含人脸图像；提取所述人脸图像的人脸特征，并将人脸特征和所述用户信息保存到用户特征库；

S200、提取视频帧的图像数据：获取源自摄像头的、安保管理范围内的实时视频，将视频进行解码，提取视频帧的图像数据；

S300、检测并提取人脸特征：对步骤S200中提取的所述视频帧的图像数据进行人脸定位，使用深度学习方法提取人脸特征；

所述人脸特征包括类间变化和类内变化，所述类间变化是指不同人之间的人脸差异；所述类内变化是指一个人在不同条件下人脸之间的差异；

S400、判断是否为照片欺骗：当检测到的人脸周围连续若干帧的变化小于预设值时，则进一步从人脸位置向下扩展并对该扩展区域进行人体检测；若存在人体，则进入步骤S500；否则给出报警提示；

S500、判断是否为合法用户：将检测到的人脸特征和用户特征库进行比对判断；当为合法用户时，则允许通过；否则给出报警提示。

2.根据权利要求1所述的方法，其特征在于，步骤S300中所述定位通过采用adaboost机器学习方法来定位图像中的人脸位置。

3.根据权利要求1所述的方法，其特征在于，所述深度学习方法使用非线性变换sigmoid函数：

$$S(x)=\frac{1}{1+e^{-x}}。$$

4.根据权利要求1所述的方法，其特征在于，所述S300中的不同条件包括表情、光线、年龄所相关的条件。

5.根据权利要求1所述的方法，其特征在于，所述步骤S300之后，步骤S400之前，还包括：

S301、对定位的人脸进行位置的跟踪；

S302、判断所定位的人脸与当前跟踪位置处的人脸是否为同一目标。

6.根据权利要求5所述的方法，其特征在于，所述步骤S302通过比较当前跟踪位置处的人脸与步骤S300中已定位的人脸的面积重合度来判断是否为同一目标。

7.根据权利要求5所述的方法，其特征在于，所述步骤S302之后，步骤S400之前，还包括：

S303、当判断当前跟踪位置处的人脸与步骤S300中已定位的人脸是同一目标时，利用检测的结果修订跟踪结果。

8.根据权利要求5所述的方法，其特征在于，所述步骤S302之后，步骤S400之前，还包括：

S304、当判断当前跟踪位置处的人脸与步骤S300中已定位的人脸不是同一目标时，则认为当前跟踪位置处的人脸是新的人脸，并进一步增加对新的人脸进行跟踪。

9.根据权利要求1所述的方法，其特征在于，所述报警提示的内容形式包括采用下述一种或任意多种方式的组合形式：静态文字、图案或动态文字、动态图案、声音。

10.根据权利要求1所述的方法，其特征在于，所述步骤S300之后，步骤S400之前，还包括：

S3001、在提取到人脸特征之后还包括将检测到的人脸图像、提取到的人脸特征以及图像获取时间、地点进行存储。

11.一种基于人脸识别的安保管理系统，其特征在于，所述系统包括下述模块：

M100、用户特征库模块：收集允许通过门禁的合法用户的用户信息，所述用户信息包含人脸图像；提取所述人脸图像的人脸特征，并将人脸特征和所述用户信息保存到用户特征库；

M200、视频帧图像数据提取模块：用于在摄像头采集到安保管理范围内的实时视频之后，将视频进行解码，提取视频帧的图像数据并将其传递给模块M300；

M300、人脸特征提取模块：所述人脸特征提取模块使用图像接收单元接收模块M200中提取的视频帧的图像数据，通过人脸定位单元将接收的图像中的人脸进行定位，然后使用人脸特征提取单元采用深度学习方法提取人脸特征；

所述人脸特征包括类间变化和类内变化，所述类间变化是指不同人之间的人脸差异；

所述类内变化是指一个人在不同条件下人脸之间的差异；

M400、照片欺骗判断模块：当检测到的人脸周围连续若干帧的变化小于预设值时，则进一步从人脸位置向下扩展并对该扩展区域进行人体检测；若存在人体，则将流程转向模块M500；否则给出报警提示；

M500、合法用户判断模块：将检测到的人脸特征和用户特征库进行比对判断；当为合法用户时，则允许通过；否则给出报警提示。

12.根据权利要求11所述的系统，其特征在于，所述人脸定位单元通过采用adaboost机器学习方法来定位图像中的人脸位置。

13.根据权利要求11所述的系统，其特征在于，所述深度学习方法使用非线性变换sigmoid函数，即：

$$S(x)=\frac{1}{1+e^{-x}}。$$

14.根据权利要求11所述的系统，其特征在于，所述不同条件包括表情、光线、年龄所相关的条件。

15.根据权利要求11所述的系统，其特征在于，所述模块M300还包括人脸跟踪单元，用于在人脸定位单元定位到人脸的位置之后，判断当前跟踪位置处的人脸与所定位的人脸是否为同一目标。

16.根据权利要求15所述的系统，其特征在于，所述人脸跟踪单元通过比较当前跟踪位置处的人脸与人脸定位单元中所定位的人脸的面积重合度来判断是否为同一目标。

17.根据权利要求16所述的系统，其特征在于，所述系统在判断当前跟踪位置处的人脸与人脸定位单元中所定位的人脸是同一目标时，利用检测的结果修订跟踪结果。

18.根据权利要求16所述的系统，其特征在于，所述系统在判断当前跟踪位置处的人脸与人脸定位单元中所定位的人脸不是同一目标时，则认为当前跟踪位置处的人脸是新的人脸，并进一步增加对新的人脸进行跟踪。

19.根据权利要求11所述的系统，其特征在于，所述报警提示的内容形式包括采用下述

一种或任意多种方式的组合形式:静态文字、图案或动态文字、动态图案、声音。

20.根据权利要求11所述的系统,其特征在于,所述模块M300在提取到人脸特征之后,将检测到的人脸图像、提取到的人脸特征以及图像获取时间、地点进行存储。

一种基于人脸识别的安保管理方法及系统

技术领域

[0001] 本公开涉及门禁管理领域，特别是一种基于人脸识别的安保管理方法及系统。

背景技术

[0002] 深度学习是近十年来人工智能领域取得的最重要的突破之一。它在语音识别、自然语言处理、计算机视觉、图像与视频分析、多媒体等诸多领域都取得了巨大成功，随着互联网技术的日益更新的不断发展，数字化、网络化、智能化使生活水平更不断提高，其中智能小区管理是其中重要的一环，现有的小区物业管理大部分工作需要人力来完成，我们可以通过深度学习技术赋予摄像头“慧眼识人”的功能，来解决现有小区的安保管理中存在的问题，比如：现有小区通常需要刷卡授权出入，这不仅需要住户主动配合，而且需随身携带门卡。再比如：现有的基于人脸识别的安保管理系统不能避免照片欺骗，即若有恶意用户想恶意进入安保管理区域，可以使用被仿冒者的照片来进行恶意攻击。而在解决现有问题的同时，还可以提供更多的功能服务，比如进行人脸搜索，不仅可以定位陌生人，而且可以帮助应用本公开方法或系统的安保管理人员查找辖区范围内人员的出入记录，比如应用于小区，帮助查找住户小孩的出入记录，还可以为统计安保管理区域内的人流情况等等。

发明内容

[0003] 针对上述部分问题，本公开提供了一种基于人脸识别的安保管理方法及系统，所述方法及系统不仅可以用于普通小区管理，还可以用于其它需要门禁管理或门禁和内部均需要监控管理的地方，比如保密机构，公司，政府等等。所述方法采用深度学习来识别人脸，可以提供人脸识别的准确度。所述系统基于所述方法实现，为安保管理带来方便。

[0004] 一种基于人脸识别的安保管理方法，所述方法包括下述步骤：

[0005] S100、建立用户特征库：收集允许通过门禁的合法用户的用户信息，所述用户信息包含人脸图像；提取所述人脸图像的人脸特征，并将人脸特征和所述用户信息保存到用户特征库；

[0006] S200、提取视频帧的图像数据：获取摄像头在安保管理范围内的实时视频，将视频进行解码，提取视频帧的图像数据；

[0007] S300、检测并提取人脸特征：对步骤S200中提取的所述视频帧的图像数据进行人脸定位，使用深度学习方法提取人脸特征；

[0008] 所述人脸特征包括类间变化和类内变化，所述类间变化是指不同人之间的人脸差异；所述类内变化是指一个人在不同条件下人脸之间的差异；

[0009] S400、判断是否为照片欺骗：当检测到的人脸周围连续若干帧的变化小于预设值时，则进一步从人脸位置向下扩展并对该扩展区域进行人体检测；若存在人体，则进入步骤S500；否则给出报警提示；

[0010] S500、判断是否为合法用户：将检测到的人脸特征和用户特征库进行比对判断；当为合法用户时，则允许通过；否则给出报警提示。

[0011] 基于所述方法，实现了相应的系统，即一种基于人脸识别的安保管理系统，所述系统包括下述模块：

[0012] M100、用户特征库模块：收集允许通过门禁的合法用户的用户信息，所述用户信息包含人脸图像；提取所述人脸图像的人脸特征，并将人脸特征和所述用户信息保存到用户特征库；

[0013] M200、视频帧图像数据提取模块：用于在摄像头采集到安保管理范围内的实时视频之后，将视频进行解码，提取视频帧的图像数据并将其传递给模块M300；

[0014] M300、人脸特征提取模块：所述人脸特征提取模块使用图像接收单元接收模块M200中提取的视频帧的图像数据，通过人脸定位单元将接收的图像中的人脸进行定位，然后使用人脸特征提取单元采用深度学习方法提取人脸特征；

[0015] 所述人脸特征包括类间变化和类内变化，所述类间变化是指不同人之间的人脸差异；

[0016] 所述类内变化是指一个人在不同条件下人脸之间的差异；

[0017] M400、照片欺骗判断模块：当检测到的人脸周围连续若干帧的变化小于预设值时，则进一步从人脸位置向下扩展并对该扩展区域进行人体检测；若存在人体，则将流程转向模块M500；否则给出报警提示；

[0018] M500、合法用户判断模块：将检测到的人脸特征和用户特征库进行比对判断；当为合法用户时，则允许通过；否则给出报警提示。

[0019] 本公开具有无接触，交互自然的特点。当恶意用户使用照片欺骗，即使用被仿冒者的照片以求进入安保管理区域，系统发现则实时提醒门卫，并给对应的用户发送警告消息。本公开系统可以进行人脸搜索，不仅可以定位陌生人，而且可以帮助应用本公开方法或系统的安保管理人员查找辖区范围内人员的出入记录，比如应用于小区，帮助查找住户小孩的出入记录，还可以为统计安保管理区域内的人流情况等等。

附图说明

[0020] 图1本公开的一个实施例中的一种基于人脸识别的安保管理方法流程图。

具体实施方式

[0021] 在一个基础的实施例中，提供了一种基于人脸识别的安保管理方法，所述方法包括下述步骤：

[0022] S100、建立用户特征库：收集允许通过门禁的合法用户的用户信息，所述用户信息包含人脸图像；提取所述人脸图像的人脸特征，并将人脸特征和所述用户信息保存到用户特征库；

[0023] S200、提取视频帧的图像数据：获取摄像头在安保管理范围内的实时视频，将视频进行解码，提取视频帧的图像数据；

[0024] S300、检测并提取人脸特征：对步骤S200中提取的所述视频帧的图像数据进行人脸定位，使用深度学习方法提取人脸特征；

[0025] 所述人脸特征包括类间变化和类内变化，所述类间变化是指不同人之间的人脸差异；所述类内变化是指一个人在不同条件下人脸之间的差异；

[0026] S400、判断是否为照片欺骗：当检测到的人脸周围连续若干帧的变化小于预设值时，则进一步从人脸位置向下扩展并对该扩展区域进行人体检测；若存在人体，则进入步骤S500；否则给出报警提示；

[0027] S500、判断是否为合法用户：将检测到的人脸特征和用户特征库进行比对判断；当为合法用户时，则允许通过；否则给出报警提示。

[0028] 在这个实施例中，所述用户信息至少包括人脸图像和通信方式，其中通信方式方便在发生照片欺骗时通知被仿者。所述人脸图像的获取方式可以是在线拍摄，也可以是提供照片上传的方式。优选的，要求人脸图像包含完整正脸的清晰照片，像素值在180*240以上，且两眼距离在35个像素点以上。这样保证人脸能够有效精准地被识别。

[0029] 由于在手机或者pad等设备上用来欺骗的人脸照片具有如下特点：

[0030] (1)人脸包含在手机或pad等设备的外部矩形框内；

[0031] (2)由于照片大小有限，无完整的人体三维形状；

[0032] 因此，如果检测的人脸周围连续若干帧基本无变化，比如2帧，就可以进一步从人脸位置向下扩展，检验该区域是否存在人体，通过这种方式来避免他人使用照片方式来进行欺骗进入安保管理区域。

[0033] 优选的，所述人体检测使用HOG人体检测算法。这里优选使用HOG人体检测算法的原因在于在一幅图像中，局部目标的表象和形状能够被梯度或边缘的方向密度分布很好地描述。所述HOG人体检测算法包括下述步骤：

[0034] S401、将图像分成小的连通区域，这些小的连通区域被称为细胞单元；

[0035] S402、采集细胞单元中各像素点的梯度的或边缘的方向直方图；

[0036] S403、将这些直方图组合起来构成特征描述器。

[0037] 在步骤S400中，若检测出照片欺骗，则可以向监管人员给出报警提示，同时给被仿者发出通知。

[0038] 在一个实施例中，所述人脸图像在用于检测并提取人脸特征之前，进行图像预处理，以减少不同光照下对人脸识别效果的影响，比如进行直方图均衡化、Gamma灰度校正等。

[0039] 优选的，给出了一种人脸定位的具体方法，即：步骤S300中所述定位通过采用adaboost机器学习方法来定位图像中的人脸位置。

[0040] 在一个实施例中，通过使用大量人脸图像和非人脸图像作为图像样本提取haar特征，采用adaboost机器学习方法离线训练haar特征，自动选择合适的haar特征组合成强分类器，把要检测的人脸图像输入强分类器进行遍历即可进行人脸定位。haar特征是基于灰度图，因此在进行人脸图像检测之前，先将图像处理成灰度图。在训练强分类器时，首先通过大量的具有比较明显的haar特征(矩形)的物体图像用模式识别的方法训练出分类器，分类器是个级联的，每级都以大概相同的识别率保留进入下一级的具有物体特征的候选物体，而每一级的子分类器则由许多haar特征构成(由积分图像计算得到，并保存下位置)，有水平的、竖直的、倾斜的，并且每个特征带一个阈值和两个分支值，每级子分类器带一个总的阈值。识别人脸的时候，同样计算积分图像为后面计算haar特征做准备，然后采用与训练的时候有人脸的窗口同样大小的窗口遍历整幅图像，以后逐渐放大窗口，同样做遍历搜索物体；每当窗口移动到一个位置，即计算该窗口内的haar特征，加权后与分类器中haar特征的阈值比较从而选择左或者右分支值，累加一个级的分支值与相应级的阈值比较，大于该

阈值才可以通过进入下一轮筛选。当通过所有的分类器级的时候说明这个人脸以大概率被识别。

[0041] 优选的，给出了深度学习采用的具体函数，即：所述深度学习方法使用非线性变换sigmoid函数，即：

[0042] $S(x)=\frac{1}{1+e^{-x}}$。

[0043] 由于在不同条件下产生的类内变化与由于不同人脸产生的类间变化，这两种变化分布式非线性的且极为复杂，传统的线性模型无法将它们有效的区分开。然而，深度学习方法可以通过非线性变换得到新的特征表示：该特征在尽可能多地去掉类内变化的同时，保留类间变化。通过深度学习方法提取每张人脸个性化的特征，能很大提高人脸识别的准确性。

[0044] 在一个实施例中，列举了产生类内变化的不同条件，即：所述S300中的不同条件包括表情、光线、年龄所相关的条件。在其它实施例中，不同条件包括表情、光线、年龄、发型、化妆与否等相关的条件。

[0045] 在一个实施例中，所述步骤S300之后，步骤S400之前，还包括：

[0046] S301、对定位的人脸进行位置的跟踪；

[0047] S302、判断所定位的人脸与当前跟踪位置处的人脸是否为同一目标。

[0048] 在这个实施例中，当检测不到人脸时，能够通过跟踪这一功能保证检测目标被持续跟踪到。在记录下跟踪的时间和地点之后，可以得到检测目标的轨迹信息，而且可以根据轨迹上的不同人脸照片，无论正脸、左脸还是右脸等等，可以在所述不同人脸照片的基础上，综合得到一个更加全面的目标特征。在多个摄像头的情况下，利用每个摄像头检测的目标轨迹，比对目标特征是否匹配，还能够进行跨多摄像头跟踪。

[0049] 可选的，所述步骤S302通过比较当前跟踪位置处的人脸与步骤S300中已定位的人脸的面积重合度来判断是否为同一目标。在一个实施例中，比较所定位的人脸与当前跟踪位置处的“人脸”的面积重合度，如果重合度大于阈值，比如0.6，则认为是同一个目标，如果所定位的人脸没有与跟踪的人脸重合或者重合度小于阈值，则认为不是同一目标。

[0050] 在一个实施例中，所述步骤S302之后，步骤S400之前，还包括：

[0051] S303、当判断当前跟踪位置处的人脸与步骤S300中已定位的人脸是同一目标时，利用检测的结果修订跟踪结果。

[0052] 在一个实施例中，所述步骤S302之后，步骤S400之前，还包括：

[0053] S304、当判断当前跟踪位置处的人脸与步骤S300中已定位的人脸不是同一目标时，则认为当前跟踪位置处的人脸是新的人脸，并进一步增加对新的人脸进行跟踪。

[0054] 可选的，所述报警提示的内容形式包括采用下述一种或任意多种方式的组合形式：静态文字、图案或动态文字、动态图案、声音。所述报警提示可以采用的设备包括使用图像显示设备、声音报警装置等装置来实现。

[0055] 可选的，所述步骤S300之后，步骤S400之前，还包括：

[0056] S3001、在提取到人脸特征之后还包括将检测到的人脸图像、提取到的人脸特征以及图像获取时间、地点进行存储。

[0057] 这里可以专门建立一个人脸图像数据库，已记录出现过得人脸信息，用于人脸检

索，可以得到所有相似人的所有记录。存储的数据可以方便后续备查。在查找时，用户上传一张待搜索的人脸照片，其质量与入库图片要求一致，和已存储的人脸特征进行对比，再结合时间与位置多个维度来搜索，可以将出入历史记录报考截图、时间等检索出来。在一个实施例中，利用存储的数据进行人脸搜索，帮助应用本公开方法的小区住户查找小孩的出入记录。在一个实施例中，利用存储的数据统计门禁处人员出入情况，进一步估算安保管理区域的人流数据。在一个实施例中，对陌生人的出入进行定位。

[0058] 下面结合附图1阐述本公开的方法。

[0059] 如图1所示，建立用户特征库时，先采集允许通过门禁的合法用户的人脸图像，并对图像进行预处理，然后进行人脸检测和人脸特征提取，并将包括人脸图像、人脸特征以及其对应的用户信息存储到用户特征库中以备使用。在门禁处通过摄像头采集视频源，在经过视频解码、图像预处理、人脸检测与跟踪、人脸特征提取之后，将采集的图像、提取的人脸特征以及图像获取时间、地点等信息存储到人脸图像数据库中，以备人脸检索，从而可以得到所有相似人的所有记录。在进行特征提取之后，紧接着需要进行照片检测，以防恶意人员使用照片欺骗。当检测出是照片是，则在保安显示界面给出报警提示；否则，到用户特征库中进行检索，与用户特征进行比对，以判断是否为合法用户；如果是，则开门；否则，在保安显示界面给出报警提示。可选的，所述报警提示的内容形式包括采用下述一种或任意多种方式的组合形式：静态文字、图案或动态文字、动态图案、声音。所述报警提示可以采用的设备包括使用图像显示设备、声音报警装置等装置来实现。

[0060] 基于上述方法，在一个实施例中实现了一种基于人脸识别的安保管理系统，所述系统包括下述模块：

[0061] M100、用户特征库模块：收集允许通过门禁的合法用户的用户信息，所述用户信息包含人脸图像；提取所述人脸图像的人脸特征，并将人脸特征和所述用户信息保存到用户特征库；

[0062] M200、视频帧图像数据提取模块：用于在摄像头采集到安保管理范围内的实时视频之后，将视频进行解码，提取视频帧的图像数据并将其传递给模块M300；

[0063] M300、人脸特征提取模块：所述人脸特征提取模块使用图像接收单元接收模块M200中提取的视频帧的图像数据，通过人脸定位单元将接收的图像中的人脸进行定位，然后使用人脸特征提取单元采用深度学习方法提取人脸特征；

[0064] 所述人脸特征包括类间变化和类内变化，所述类间变化是指不同人之间的人脸差异；

[0065] 所述类内变化是指一个人在不同条件下人脸之间的差异；

[0066] M400、照片欺骗判断模块：当检测到的人脸周围连续若干帧的变化小于预设值时，则进一步从人脸位置向下扩展并对该扩展区域进行人体检测；若存在人体，则将流程转向模块M500；否则给出报警提示；

[0067] M500、合法用户判断模块：将检测到的人脸特征和用户特征库进行比对判断；当为合法用户时，则允许通过；否则给出报警提示。

[0068] 在这个实施例中，所述用户信息至少包括人脸图像和通信方式，其中通信方式方便在发生照片欺骗时通知被仿者。所述人脸图像的获取方式可以是在线拍摄，也可以是提供照片上传的方式。优选的，要求人脸图像包含完整正脸的清晰照片，像素值在180*240以

上，且两眼距离在35个像素点以上。这样保证人脸能够有效精准地被识别。

[0069] 由于在手机或者pad等设备上用来欺骗的人脸照片具有如下特点：

[0070] (1)人脸包含在手机或pad等设备的外部矩形框内；

[0071] (2)由于照片大小有限，无完整的人体三维形状；

[0072] 因此，如果检测的人脸周围连续若干帧基本无变化，比如2帧，就可以进一步从人脸位置向下扩展，检验该区域是否存在人体，通过这种方式来避免他人使用照片方式来进行欺骗进入安保管理区域。

[0073] 优选的，所述人体检测使用HOG人体检测算法。这里优选使用HOG人体检测算法的原因在于在一幅图像中，局部目标的表象和形状能够被梯度或边缘的方向密度分布很好地描述。所述HOG人体检测算法包括下述步骤：

[0074] S401、将图像分成小的连通区域，这些小的连通区域被称为细胞单元；

[0075] S402、采集细胞单元中各像素点的梯度的或边缘的方向直方图；

[0076] S403、将这些直方图组合起来构成特征描述器。

[0077] 在模块M400中，若检测出照片欺骗，则可以向监管人员给出报警提示，同时给被仿者发出通知。

[0078] 在一个实施例中，所述人脸图像在用于检测并提取人脸特征之前，进行图像预处理，以减少不同光照下对人脸识别效果的影响，比如进行直方图均衡化、Gamma灰度校正等。

[0079] 优选的，所述人脸定位单元通过采用adaboost机器学习方法来定位图像中的人脸位置。

[0080] 在一个实施例中，通过使用大量人脸图像和非人脸图像作为图像样本提取haar特征，采用adaboost机器学习方法离线训练haar特征，自动选择合适的haar特征组合成强分类器，把要检测的人脸图像输入强分类器进行遍历即可进行人脸定位。haar特征是基于灰度图，因此在进行人脸图像检测之前，先将图像处理成灰度图。在训练强分类器时，首先通过大量的具有比较明显的haar特征(矩形)的物体图像用模式识别的方法训练出分类器，分类器是个级联的，每级都以大概相同的识别率保留进入下一级的具有物体特征的候选物体，而每一级的子分类器则由许多haar特征构成(由积分图像计算得到，并保存下位置)，有水平的、竖直的、倾斜的，并且每个特征带一个阈值和两个分支值，每级子分类器带一个总的阈值。识别人脸的时候，同样计算积分图像为后面计算haar特征做准备，然后采用与训练的时候有人脸的窗口同样大小的窗口遍历整幅图像，以后逐渐放大窗口，同样做遍历搜索物体；每当窗口移动到一个位置，即计算该窗口内的haar特征，加权后与分类器中haar特征的阈值比较从而选择左或者右分支值，累加一个级的分支值与相应级的阈值比较，大于该阈值才可以通过进入下一轮筛选。当通过所有的分类器级的时候说明这个人脸以大概率被识别。

[0081] 优选的，给出了深度学习采用的具体函数，即：所述深度学习方法使用非线性变换Sigmoid函数，即：

[0082] $S(x)=\frac{1}{1+e^{-x}}$。

[0083] 由于在不同条件下产生的类内变化与由于不同人脸产生的类间变化，这两种变化分布式非线性的且极为复杂，传统的线性模型无法将它们有效的区分开。然而，深度学习方

法可以通过非线性变换得到新的特征表示：该特征在尽可能多地去掉类内变化的同时，保留类间变化。通过深度学习方法提取每张人脸个性化的特征，能很大提高人脸识别的准确性。

[0084] 在一个实施例中，列举了产生类内变化的不同条件，即：所述不同条件包括表情、光线、年龄。在其它实施例中，不同条件包括表情、光线、年龄、发型、化妆与否等。

[0085] 在一个实施例中，所述模块M300还包括人脸跟踪单元，用于在人脸定位单元定位到人脸的位置之后，判断当前跟踪位置处的人脸与所定位的人脸是否为同一目标。在这个实施例中，当检测不到人脸时，能够通过跟踪这一功能保证检测目标被持续跟踪到。在记录下跟踪的时间和地点之后，可以得到检测目标的轨迹信息，而且可以根据轨迹上的不同人脸照片，无论正脸、左脸还是右脸等等，可以在所述不同人脸照片的基础上，综合得到一个更加全面的目标特征。在多个摄像头的情况下，利用每个摄像头检测的目标轨迹，比对目标特征是否匹配，还能够进行跨多摄像头跟踪。

[0086] 可选的，所述人脸跟踪单元通过比较当前跟踪位置处的人脸与人脸定位单元中所定位的人脸的面积重合度来判断是否为同一目标。在一个实施例中，比较所定位的人脸与当前跟踪位置处的“人脸”的面积重合度，如果重合度大于阈值，比如0.6，则认为是同一个目标，如果所定位的人脸没有与跟踪的人脸重合或者重合度小于阈值，则认为不是同一目标。在一个实施例中，所述系统在判断当前跟踪位置处的人脸与人脸定位单元中所定位的人脸是同一目标时，利用检测的结果修订跟踪结果。在一个实施例中，所述系统在判断当前跟踪位置处的人脸与人脸定位单元中所定位的人脸不是同一目标时，则认为当前跟踪位置处的人脸是新的人脸，并进一步增加对新的人脸进行跟踪。

[0087] 可选的，所述报警提示的内容形式包括采用下述一种或任意多种方式的组合形式：静态文字、图案或动态文字、动态图案、声音。所述报警提示可以采用的设备包括使用图像显示设备、声音报警装置等装置来实现。

[0088] 可选的，所述模块M300在提取到人脸特征之后，将检测到的人脸图像、提取到的人脸特征以及图像获取时间、地点进行存储。这里可以专门建立一个人脸图像数据库，已记录出现过得人脸信息，用于人脸检索，可以得到所有相似人的所有记录。存储的数据可以方便后续备查。在查找时，用户上传一张待搜索的人脸照片，其质量与入库图片要求一致，和已存储的人脸特征进行对比，再结合时间与位置多个维度来搜索，可以将出入历史记录报考截图、时间等检索出来。在一个实施例中，利用存储的数据进行人脸搜索，帮助应用本公开系统小区的住户查找小孩的出入记录。在一个实施例中，后台利用存储的数据统计门禁处人员出入情况，进一步估算安保管理区域人流数据。在一个实施例中，对陌生人的出入进行定位。

[0089] 综上，本公开提供的一种基于人脸识别的安保管理方法及系统，所述方法及系统不仅可以用于普通小区管理，还可以用于其它需要门禁管理或门禁和内部均需要监控管理的地方，比如保密机构，公司，政府等等。所述方法采用深度学习来识别人脸，可以提供人脸识别的准确度。所述系统基于所述方法实现，为安保管理带来方便。

[0090] 以上对本公开进行了详细介绍，本文中应用了具体个例对本公开的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本公开的方法及其核心思想；同时，对于本领域技术人员，依据本公开的思想，在具体实施方式及应用范围上均会有改变之处，综

上所述，本说明书内容不应理解为对本公开的限制。

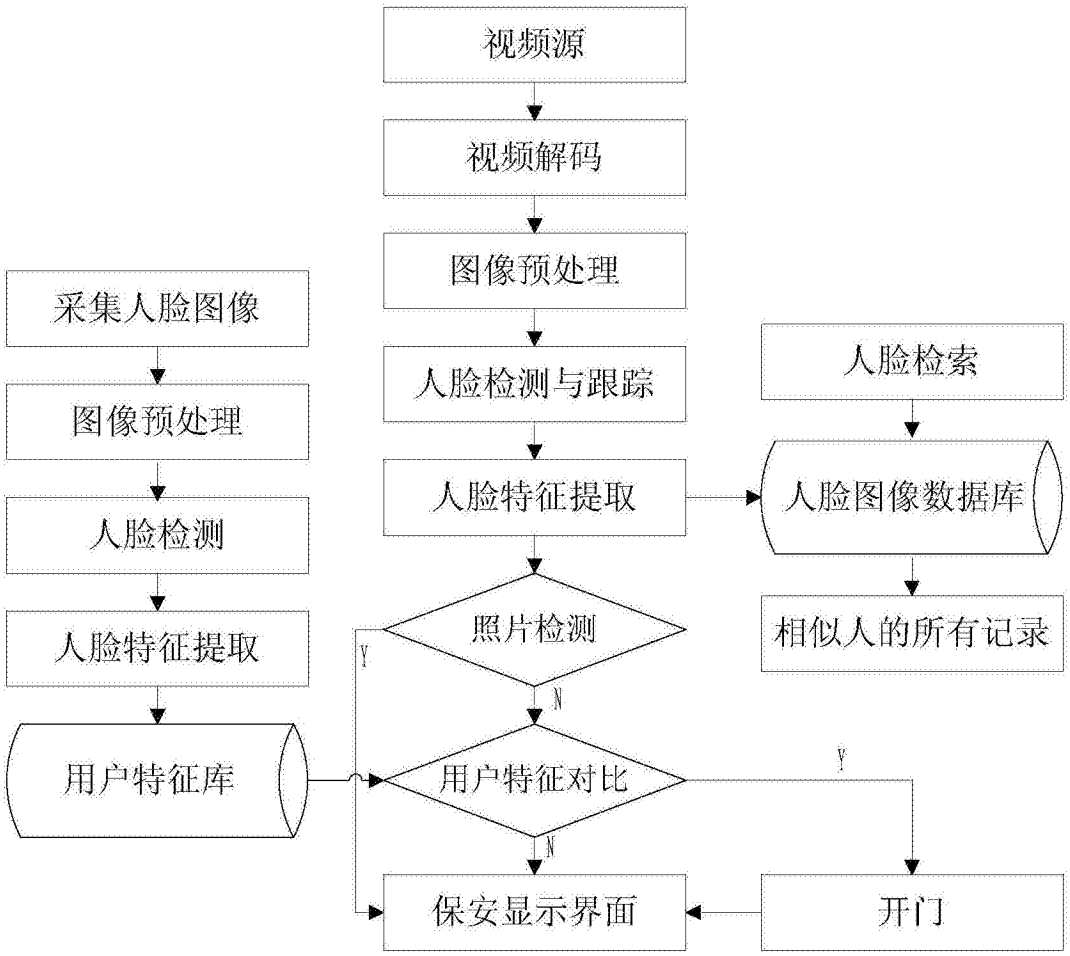

视频源
视频解码
图像预处理
人脸检测与跟踪
人脸特征提取
照片检测
用户特征对比
保安显示界面
开门
采集人脸图像
图像预处理
人脸检测
人脸特征提取
用户特征库
人脸检索
人脸图像数据库
相似人的所有记录
Y
N
Y
N

图1